MANAGING TRUST ACROSS THE ORGANIZATION

WITH DIGICERT® TRUST LIFECYCLE MANAGER

Changing Security Needs

Evolving threat landscapes and changing IT infrastructures are demanding greater attention to how companies protect users, devices, and servers and agility in responding to threats and changes in standards.

Evolving Threat Landscape with an increasing number of material breaches, software supply chain attacks, and attack vectors.

Changing IT Architectures with the move to multi-cloud workloads, convergence of IT and OT, investment in zero-trust architectures, and the need for stronger authentication measures.

Crypto-Agility that enables organizations to rapidly remediate vulnerabilities or breaches, adapt to changes in standards such as shorter certificate validity periods, and prepare for post-quantum cryptography.

Remote Work demands that have rapidly transformed infrastructure risk and need for new protocols around security for remote endpoints, digital collaboration tools, bring-your-own-devices, and always-on VPNs.

Digital Trust as a Strategic Imperative

From security teams to compliance officers, developers, and business executives, Trust Lifecycle Manager offers valuable capabilities and benefits that cater to the unique needs of each audience.

CIO/CISO

For CIOs and CISOs, Trust Lifecycle Manager provides a full-stack solution for certificate management, PKI services, and public and private trust issuance, reducing the vendors needed to support a comprehensive digital trust infrastructure. This integrated solution **reduces the risk of business disruption, protects attack surfaces, and improves security posture and cryptoagility**, delivering greater visibility and control over cryptographic assets and reducing the risk of security breaches and other potential threats.

Identity & Access Management

For Identity and Access Management managers, Trust Lifecycle Manager **improves the user experience** of certificate-mediated authentication while **improving productivity and securing identity and access**. Through its broad integration with IAM technologies, Trust Lifecycle Manager supports certificate lifecycle automation for a range of authentication needs, such as WiFi/VPN access, passwordless authentication, mobile device authentication, and more. Trust Lifecycle Manager improves adherence to security policy, enables instant remediation, and eliminates delays associated with provisioning and revocation of user access.

Infrastructure & Operations

For Infrastructure and Operations managers, Trust Lifecycle Manager **centralizes visibility and control** over certificate landscapes, **reducing the risk of unplanned certificate outages** that disrupt business and **enforcing certificate practices and security policy**. With these capabilities, organizations can avoid the high cost of downtime or audit failures, adapt quickly to changes in compliance requirements, and streamline the operational demands of increasing use cases and shorter validity periods.